FingerLakes COMMUNITY COLLEGE

Success. It's In Our Nature.

Policy Name: Computer Device Management and Use **Policy Number:** J-2

Functional Area(s) Responsible: Information Technology

Owner(s) of Policy: Information Technology

Most Recent BOT Approval Date: September 2011

Most Recent Review Date: Spring 2023

Most Recent Review/Revision Type: ☐ none ☒ minor/non-substantive ☐ substantive/extensive

Policy Statement:

Individual computing devices which utilize Finger Lakes Community College's networks must be managed and used in a manner which conforms to essential best practices. This policy does not apply to the colleges external public wifi networks.

Reason(s) for Policy:

To protect the FLCC computing environment from operational disruptions and security breaches while ensuring a quality IT environment for all users.

Applicability of Policy:

This policy applies to all individuals utilizing any device which accesses the College's internal data networks.

Definitions:

Best Practices

For the purposes of this policy, essential Best Practices consist of the following:

- All operating systems and applications software must be of a current, supported version and receiving periodic updates.
- All devices which support Anti Virus software must be equipped with an updated version of the AV software and scanned on a weekly basis for the presence of viruses and malware.
- An active program providing security patches and addressing detected viruses and malware is required for all relevant devices.
- Portable devices may access the FLCC network through wireless means only – they cannot be connected directly to hard-wired network ports except as specifically authorized by the Network Administrator.
- Users of devices on the College's networks must adhere to all relevant IT policies including the Network Usage Policy and Security of IT Systems and Data Policy.
- Local storage of data on computing devices should be synchronized with OneDrive to avoid any loss of data in case of a computer crash. Generally, it is expressly disallowed for information which is regarded as sensitive by the Security of IT Systems and Data Policy to leave a college own storage device.
- Users who are assigned individual accounts may not share those accounts under any circumstances. In addition, they are responsible for keeping their passwords secure, utilizing an alphanumeric mix with a minimum of 8 characters or longer with required use of special characters for complexity requirements. Passwords should periodically be changed.

Related Documents:

- Security of IT Systems and Data Policy
- Network Usage Policy

Procedures:

College-Owned Computing Devices

College-Owned computing devices which are college owned are those purchased through the College operating budget, technology fund, or acquired by the College through grants and gifts.

Devices managed by the IT Division

College-owned, standardized systems which are acquired through the Information Technology Division will be the responsibility of the Information Technology Division for management under this policy. Users can ensure that the IT Division is responsible for the full support and management of their computing equipment by acquiring it under the "FLCC Guidelines for Purchasing Computing Equipment and Software"

Users of IT supported computing devices should avoid the following activities – failure to do so can result in suspension of IT's management services for that device.

- Loading software on the device without prior IT approval. Requests for local admin rights are normally granted on a temporary basis for this purpose.
- In the case where specialized software is approved, the user may have to assume the responsibility for periodic updates of the software.
- Connecting peripheral devices to a college-owned device without prior approval. The IT area should be consulted in all such cases first.
- If the use of a thumb drive or other external storage device is required, it must first be encrypted before storing any college data on the device.
- Moving a desktop system to a new location (i.e. a different network port) without first consulting the IT area.
- All portable devices and laptops will have their hard drives encrypted by IT prior to release to the college community.

Other College-Owned Computing Devices

In the case of non-standard computing equipment acquired by an office or department for a specialized purpose, the office or department is the area responsible for providing the software updates, virus protection, and related system management requirements defined in this policy. Where possible, the IT Division will coordinate activities with these areas to avoid a duplication of effort.

Personally-Owned Devices

Personally owned devices are not allowed to interact with college enterprise systems as it is not possible for IT to manage their security.

Oversight of Policy Implementation

The IT area is responsible for implementation of this policy. In that effort it may inspect software loads on individual systems, examine the effectiveness of password use, monitor cases where multiple users may be logged on to a single account, and to the extent possible determine the degree of adherence to the policy across the institution. In the event that a device is identified as being non-compliant with the policy, the IT Division may deny access for the device or user's account until the problem is rectified.

Forms/Online Processes:

None

Appendix:

None